Corso - 21/11/2024

Cybersecurity applicata alle macchine e impianti

Quali obblighi, l'analisi dei rischi secondo la IEC serie 62443, le responsabilità dei fabbricanti, gli aspetti applicativi su vulnerability e test connessi.

Obiettivi

Il corso è strutturato in tre moduli, ciascuno dedicato a diversi aspetti fondamentali della sicurezza informatica e dei sistemi industriali. Il percorso è rivolto a professionisti responsabili della sicurezza IT/OT e si propone l'obiettivo di:

- comprendere l'evoluzione della sicurezza di un macchinario sempre più integrato in linee, processi e reti industriali: dal concetto tradizionale di Safety alla moderna Cybersecurity, per avere una visione chiara di come le due discipline si integrano nel contesto delle macchine industriali.
- Acquisire una conoscenza approfondita delle direttive e dei regolamenti nazionali ed internazionali in materia di sicurezza informatica, con un focus specifico su normative come il Cyber Resilience Act e la Direttiva NIS 2 e le prescrizioni del National Electrical Code 2023 americano.
- Apprendere le metodologia per effettuare la prevista analisi dei rischi secondo la 62443-3-2 e 3-3: Definizione di Protection Level, Security Level Target e Maturity Level.
- Apprendere tecniche pratiche di protezione: attraverso moduli dedicati ai test di vulnerabilità e a prove di attacco simulato, per sviluppare competenze pratiche per identificare e gestire le criticità nei sistemi informatici e industriali.

Programma

MODULO 1

21 novembre, dalle 9.00 alle 18.00, presso la sede SBS di Villa Marchetti, Baggiovara di Modena

Dalla Safety alla Cybersecurity, l'evoluzione del concetto di sicurezza nel mondo delle macchine industriali e dei sistemi robotizzati

- Lo scenario nazionale ed internazionale per la Cybersecurty, direttive, regolamenti e norme
- Il quadro legale applicabile in materia di Cybersicurezza delle Macchine: Il Regolamento macchine, il Cyber Resilience act e la direttiva NIS 2. A cura Avv. Claudio Gabriele
- La Cybersecurity nel NEC2023 e nel Nuovo Regolamento macchine, che cosa è richiesto, gli standard
- La certificazione ISA SECURE
- La differenza tra safety e security. Sinonimi o Complementari?
- Alcuni casi di Cyber Attack, ransomware e furto di dati
- Cyber Security e GDPR
- Introduzione alla sicurezza informatica (CIA)
- Obiettivi sicurezza informatica, vulnerabilità ed attacco ad un sistema, concetto di rischio
- Distinzione IT/OT e requisiti di sicurezza associati
- Definizione IT/OT, differenze e peculiarità, defence in depth
- ISO 27001 Sicurezza delle informazioni, cybersecurity e protezione della privacy - Sistemi di gestione per la sicurezza delle informazioni

Introduzione alla cybersecurity

- Elementi di Cybersecurity
- Confidenzialità, integrità e disponibilità (CIA Triad)
- Importanza delle informazioni
- Data Classification
- Le principali minacce
- Il triangolo della sicurezza AAA
- Sicurezza preventiva, predittiva e proattivi

L'analisi dei rischi secondo la ISO 62443-3-2 e 3-3: Definizione di Protection Level, Security Level Target e Maturity Level

- Struttura dello standard IEC 62443
- Introduzione al Control Systems Security
- Maturity e Security Level Definizione e descrizione dei relativi livelli
- IEC 62443-2 (Policies e procedure)
- IEC 62443-2-1 Establishing an Industrial Automation and Control System Security Program
- IEC 62443-3 (Sistema)
- IEC 62443-3-2 Security Risk Assessment and System Design
- IEC 62443-3-3 System Security Requirements and Security Levels
- L'analisi della struttura di rete, connessioni, i requisiti del software e Hardware per i SL 1, 2, 3 e 4
- Esempi pratici ed esercizi di analisi delle singole parti con la matrice di analisi dei SL.
- I componenti e sistemi , requisiti Hardware e configurazione
- IEC 62443-4 (Componenti)
- IEC 62443-4-2 Technical Security Requirements for IACS Components

Chiusura Lavori

Conclusione lavori e dibattito finale su: Le responsabilità dei fabbricanti di macchine per la violazione delle disposizioni di legge in materia di Cybersicurezza, le procedure di vigilanza del mercato.

Relatori:

Avv. Claudio Gabriele, Ing. Matteo Marconi, Avv. Maria Sole Lora

MODULO 2

9 e 11 dicembre, dalle 9.00 alle 13.00 (Online)

Vulnerability assessment

Il modulo fornisce una comprensione approfondita delle vulnerabilità informatiche, consentendo ai partecipanti di acquisire le competenze necessarie per identificare, valutare e mitigare i rischi associati.

Attraverso l'analisi della TOP 10 OWASP e l'utilizzo di sistemi di valutazione come CVE e CVSS, i partecipanti saranno in grado di stimare l'impatto potenziale delle vulnerabilità e di implementare misure di sicurezza efficaci. Il modulo si focalizzerà inoltre sullo sviluppo di abilità pratiche nella conduzione di vulnerability assessment e nella comprensione dei risultati delle analisi.

- Introduzione alle vulnerabilità
- La TOP 10 OWASP
- Stima di una vulnerabilità (CVE e CVSS)
- Vulnerability Assessment
- Il processo di VA
- Tipologie di scansioni
- Vulnerability Analysis
- Laboratorio

Relatori:

Docenti di Tinexta Cyber S.P.A.

MODULO 3

16 e 18 dicembre, dalle 9.00 alle 13.00 (Online)

Penetration Test

Il modulo offre una panoramica completa del processo di penetration testing, dalla fase iniziale di raccolta informazioni fino alla redazione del report finale. I partecipanti impareranno a seguire una metodologia rigorosa per identificare le debolezze nei sistemi informatici, valutare il rischio associato e proporre soluzioni efficaci per mitigare le vulnerabilità.

- Introduzione al Penetration test
- Penetration Test Framework
- Le fasi di un Penetration test

  Engagement
  Footprinting

Scanning
Enumeration
Vulnerability Analysis
Exploitation
Post-exploitation
Reporting

- Laboratorio

Relatori:
Docenti di Tinexta Cyber S.P.A.

Ulteriori informazioni
La quota di partecipazione è comprensiva di materiale didattico in formato digitale, attestato di partecipazione in formato digitale e pranzo. di lavoro per la giornata del 21 novembre.

Destinatari
RSPP e ASPP, Responsabile manutenzione, Responsabile produzione, Responsabile Formazione, Responsabili IT, Responsabili OT, programmatori di PLC, Uffici Tecnici aziendali e Innovation manager.

Durata
24 ore

Quota di adesione:
1.200,00 € + IVA a persona per le aziende associate
1.500,00 € + IVA a persona per le aziende non associate

Date e Sedi di svolgimento
21/11/2024 09.00-18.00 - Modena
09/12/2024 09.00-13.00 - ONLINE
11/12/2024 09.00-13.00 - ONLINE
16/12/2024 09.00-13.00 - ONLINE
18/12/2024 09.00-13.00 - ONLINE

Allegati

» Brochure